UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,106	07/24/2007	Fabien Thomas	CU-5118 BWH	8912

26530 7590 07/31/2009

LADAS & PARRY LLP
224 SOUTH MICHIGAN AVENUE
SUITE 1600
CHICAGO, IL 60604

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2434	
MAIL DATE	DELIVERY MODE
07/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/594,106	THOMAS ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 September 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/23/2009 has been entered.

2. Independent Claims 1 and 6 are amended.

3. **Claims 1-12** are pending.

Response to Arguments

4. Applicant's arguments with respect to pending claims have been considered but are moot in view of the new ground(s) of rejection.

Drawings

5. **FIG.5** is objected to under 37 CFR 1.83(a) because it fails to show stage '**100**' as described in the specification (see page 9, lines 36-38). Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and

informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2 and 5-12 rejected under 35 U.S.C. 103(a) as being unpatentable over Zuk et al. (US 2003/0154399 A1 – "Zuk") in view of Holland, III et al. (US 6,851,061 B1 – "Holland")

As per Claim 1, Zuk teaches,

A method for the detection and prevention of intrusions into a computer network with a firewall, the method comprising: detecting the connections at a central point [see **MMIDP central management server 30** in FIG.2] and before each branch of said network [see FIG.2], selective filtering of the said connections [see at least FIGS.6 and 9], where said selective filtering stage includes firstly a stage for automatic recognition of the accessing protocol [see **Protocol Anomaly Detection Software Module 130** in FIG.6], independently of the communication port used by the said protocol [see FIG.9], and secondly, after said accessing protocol has been recognized automatically [see **Determine protocols associated to the packet flow and session 220** in FIG.9], a stage for verifying the conformity of each communication flowing in a given connection to the said protocol [see **Query protocol database for relevant protocol specification 225** in FIG.9], to deliver a dynamic authorization for communications resulting from normal operation of the protocol [see **Matching specifications? = Y** in FIG.9] and to deliver a dynamic rejection for communications resulting from abnormal operation of the protocol [see **Drop packets 235** in FIG.9. See also FIG.13: where packets are **dropped if protocol irregularities** are found in the packets], and wherein said check on conformity is performed layer by layer [see FIGS.7 and

13], by successive protocol analysis of each part of the data packet flowing in the connection corresponding to a given protocol [see **Flow Manager Software Module 120** in FIG.6], from the lowest protocol to the highest protocol [see at least FIG.10: protocol stack is disclosed].

Zuk discloses **MMIP sensor** organizing packets into FTP flow when the user's IP address is different from address of the FTP server [see at least FIG.16]; but does not explicitly disclose wherein, since each main connection enabled is able to induce one or more secondary connections, said check on conformity detects the data necessary for opening said secondary connections and dynamically attaches said secondary connections to the authorization for connection of said main connection. However, in the same field of endeavor, **Holland** discloses this limitation [see at least abstract; and FIGS.4-7: where **Holland** discloses a protocol stack **multiplexor** capable of switching, redirecting and/or opening connections]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of applicant's invention was made, to combine the teachings of **Zuk** and **Holland** and arrived at the claimed invention. The modification is beneficial to efficiently detect network intrusions [see at least abstract of **Holland**].

As per Claim 6, Zuk-Holland combination teaches,

A device for the detection and prevention of intrusions into a computer network, comprising: a firewall [see **Firewall 85b** in FIG.3; and for example, par.0085 and par.0046 of **Zuk** that discloses "*...MMIDP system may be used by itself or in conjunction with a firewall*"], a resource for preventing intrusions by detection of the connections, directly incorporated into said firewall at a central point and before each branch of said network [see **MMIDP central management server 30** in FIG.2 of **Zuk**], where said resource for the prevention of intrusions includes a resource for selective filtering of said connections by automatic recognition of the accessing protocol [see at least FIGS.6 and 9 of **Zuk**], independently of the communication port used by said protocol [see FIG.9 of **Zuk**], wherein said selective filtering resource includes at least one independent module for the analysis of at least one given communication protocol [see **Protocol Anomaly Detection Software Module 130** in FIG.6 of **Zuk**], and at least one of the

independent modules includes: (i). unit for the automatic recognition of a given communication protocol [see **Determine protocols associated to the packet flow and session 220** in FIG.9 of **Zuk**], (ii). unit for verifying the conformity of the communication flowing in a given connection to the said protocol [see **Query protocol database for relevant protocol specification 225** in FIG.9 of **Zuk**], (iii). means for delivering a dynamic authorization for communications resulting from normal operation of the protocol [see **Matching specifications? = Y** in FIG.9 of **Zuk**], and delivering a dynamic rejection for communications resulting from abnormal operation of the protocol [see **Drop packets 235** in FIG.9 and FIG.13 of **Zuk**], and (iv). means of transmission of a part of a data packet to an independent analysis module of a hierarchically higher protocol [see **Flow Manager Software Module 120** in FIG.6 and FIG.10 of **Zuk**], and wherein said unit for verifying the conformity of the communication flowing in a given connection, called main connection, to the said protocol, comprising means of detection of the data necessary for opening secondary connections induced by said main connection, and of attachment of said secondary connections to the authorization for connection of said main connection [see at least FIG.16 of **Zuk** with at least abstract; and FIGS.4-7 of **Holland**].

As per Claim 2, Zuk-Holland combination teaches,

A method according to claim 1, wherein, as long as the accessing protocol of a connection is not recognized, the data are accepted but not transmitted [in both systems of **Zuk** and **Holland** data, or packets, are accepted regardless of connection protocol and are transmitted after intrusion analysis: see for example, FIGS.9, 11, 13 and 15 of **Zuk**]

As per Claim 5, Zuk-Holland combination teaches,

A method according to claim 2, wherein, when the accessing protocol of a connection is not automatically recognized [see at least FIG.9 of **Zuk**], said step of-checking on conformity of each communication flowing in a given connection to said protocol is replaced by a step of generic checking of coherence of data packets [see at least FIG.16 of **Zuk** with at least abstract; and FIGS.4-7 of **Holland**].

As per Claim 7, Zuk-Holland combination teaches,

A device according to claim 6, wherein, in addition to the independent module or modules for the analysis of a given communication protocol the device includes an independent generic module which attaches itself to the connections for which the protocol has been recognized by none of the other said independent modules [see at least FIG.16 of **Zuk** with at least abstract; and FIGS.4-7 of **Holland**].

As per Claims 8-11, Zuk-Holland combination teaches,

A device according to claim 6, wherein the device includes an interface for entry, by a user [see at least FIG.14: where **Zuk** discloses **GUI**], of the criteria that determine the filtering policy; wherein, said interface receives the criteria specified in natural language by the user; wherein said criteria specified in natural language include at least one protocol name; and wherein said interface allows the activation or deactivation of each of said independent modules [see for example, par.0117 and 0118: where **Zuk** details FIG.14such as filtering policy].

As per Claim 12, Zuk-Holland combination teaches,

A device according to claim 6, wherein the device includes a resource for statistical processing of the connection data, and a resource for storage of said connection data and processed data [see at least **MMIDP database 35** in FIG.2 of **Zuk**].

Claims 3 and 4 rejected under 35 U.S.C. 103(a) as being unpatentable over "Zuk" in view of "Holland", further in view of Ormazabal et al. (US 7,076,393 B2 – "Ormazabal")

As per Claims 3 and 4, Zuk-Holland combination teaches,

A method according to claim 2, and **Zuk** discloses monitoring Signature counts threshold [see at least FIGS.12 and 13]; but does not explicitly disclose wherein, if the number of data packets accepted but not transmitted exceeds a certain threshold, or if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection is considered not to have been analyzed; and wherein if the data are accepted but not transmitted for a time exceeding a certain threshold, then the connection

is considered not to have been analyzed. Nevertheless, in the same filed of endeavor, **Ormazabal** monitoring the time threshold of transmission [see at least FIGS.5B and 9]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of applicant's invention was made, to modify the **Zuk-Holland** combination by incorporating the teaching of **Ormazabal** in order to quantify network vulnerability [see at least abstract of **Ormazabal**].

CONTACT INFORMATION

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **AMARE TABOR** whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Kambiz Zand** can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2434)

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434